EXHIBIT A-1

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

STATE OF MINNESOTA **DISTRICT COURT**

COUNTY OF HENNEPIN **FOURTH JUDICIAL DISTRICT**

ROBERT SMITHBURG, THOMAS LINDSAY, and ROBIN GUERTIN, individually and on behalf of all others similarly situated, Plaintiffs, v. APPLE VALLEY MEDICAL CLINIC, LTD., ALLINA HEALTH SYSTEM, SANDHILLS MEDICAL FOUNDATION, INC., and NETGAIN TECHNOLOGY, LLC, Defendants.	Court File No.: _____ **SUMMONS**

THIS SUMMONS IS DIRECTED TO NETGAIN TECHNOLOGY, LLC.

1. YOU ARE BEING SUED. The Plaintiffs have started a lawsuit against you. The Plaintiffs' Complaint against you is attached to this summons. Do not throw these papers away. They are official papers that affect your rights. You must respond to this lawsuit even though it may not yet be filed with the Court and there may be no court file number on this summons.

2. YOU MUST REPLY WITHIN 21 DAYS TO PROTECT YOUR RIGHTS. You must give or mail to the person who signed this summons **a written response** called an Answer within 21 days of the date on which you received this Summons. You must send a copy of your Answer to the person who signed this summons located at:

Raina C. Borrelli
Turke & Strauss LLP
613 Williamson St., Suite 201
Madison, WI 53703
raina@turkestrauss.com

3. YOU MUST RESPOND TO EACH CLAIM. The Answer is your written response to the Plaintiff's Complaint. In your Answer you must state whether you agree or disagree with each paragraph of the Complaint. If you believe the Plaintiff should not be given everything asked for in the Complaint, you must say so in your Answer.

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

4. YOU WILL LOSE YOUR CASE IF YOU DO NOT SEND A WRITTEN RESPONSE TO THE COMPLAINT TO THE PERSON WHO SIGNED THIS SUMMONS. If you do not Answer within 21 days, you will lose this case. You will not get to tell your side of the story, and the Court may decide against you and award the Plaintiffs everything asked for in the complaint. If you do not want to contest the claims stated in the complaint, you do not need to respond. A default judgment can then be entered against you for the relief requested in the complaint.

5. LEGAL ASSISTANCE. You may wish to get legal help from a lawyer. If you do not have a lawyer, the Court Administrator may have information about places where you can get legal assistance. **Even if you cannot get legal help, you must still provide a written Answer to protect your rights or you may lose the case**.

6. ALTERNATIVE DISPUTE RESOLUTION. The parties may agree to or be ordered to participate in an alternative dispute resolution process under Rule 114 of the Minnesota General Rules of Practice. You must still send your written response to the Complaint even if you expect to use alternative means of resolving this dispute.

/s/ Raina C. Borrelli _____ 6/15/2021 _____
Plaintiffs' attorney's signature Dated

Raina C. Borrelli _____
Print or type plaintiffs' attorney's name

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

STATE OF MINNESOTA **DISTRICT COURT**

COUNTY OF HENNEPIN **FOURTH JUDICIAL DISTRICT**

ROBERT SMITHBURG, THOMAS LINDSAY, and ROBIN GUERTIN, individually and on behalf of all others similarly situated, Plaintiffs, v. APPLE VALLEY MEDICAL CLINIC, LTD., ALLINA HEALTH SYSTEM, SANDHILLS MEDICAL FOUNDATION, INC., and NETGAIN TECHNOLOGY, LLC, Defendants.	Court File No.: _____ **SUMMONS**

THIS SUMMONS IS DIRECTED TO SANDHILLS MEDICAL FOUNDATION, INC.

1. YOU ARE BEING SUED. The Plaintiffs have started a lawsuit against you. The Plaintiffs' Complaint against you is attached to this summons. Do not throw these papers away. They are official papers that affect your rights. You must respond to this lawsuit even though it may not yet be filed with the Court and there may be no court file number on this summons.

2. YOU MUST REPLY WITHIN 21 DAYS TO PROTECT YOUR RIGHTS. You must give or mail to the person who signed this summons **a written response** called an Answer within 21 days of the date on which you received this Summons. You must send a copy of your Answer to the person who signed this summons located at:

Raina C. Borrelli
Turke & Strauss LLP
613 Williamson St., Suite 201
Madison, WI 53703
raina@turkestrauss.com

3. YOU MUST RESPOND TO EACH CLAIM. The Answer is your written response to the Plaintiff's Complaint. In your Answer you must state whether you agree or disagree with each paragraph of the Complaint. If you believe the Plaintiff should not be given everything asked for in the Complaint, you must say so in your Answer.

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

4. YOU WILL LOSE YOUR CASE IF YOU DO NOT SEND A WRITTEN RESPONSE TO THE COMPLAINT TO THE PERSON WHO SIGNED THIS SUMMONS. If you do not Answer within 21 days, you will lose this case. You will not get to tell your side of the story, and the Court may decide against you and award the Plaintiffs everything asked for in the complaint. If you do not want to contest the claims stated in the complaint, you do not need to respond. A default judgment can then be entered against you for the relief requested in the complaint.

5. LEGAL ASSISTANCE. You may wish to get legal help from a lawyer. If you do not have a lawyer, the Court Administrator may have information about places where you can get legal assistance. **Even if you cannot get legal help, you must still provide a written Answer to protect your rights or you may lose the case**.

6. ALTERNATIVE DISPUTE RESOLUTION. The parties may agree to or be ordered to participate in an alternative dispute resolution process under Rule 114 of the Minnesota General Rules of Practice. You must still send your written response to the Complaint even if you expect to use alternative means of resolving this dispute.

/s/ Raina C. Borrelli _____ 6/15/2021 _____
Plaintiffs' attorney's signature Dated

Raina C. Borrelli _____
Print or type plaintiffs' attorney's name

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

STATE OF MINNESOTA **DISTRICT COURT**

COUNTY OF HENNEPIN **FOURTH JUDICIAL DISTRICT**

ROBERT SMITHBURG, THOMAS LINDSAY, and ROBIN GUERTIN, individually and on behalf of all others similarly situated, Plaintiffs, v. APPLE VALLEY MEDICAL CLINIC, LTD., ALLINA HEALTH SYSTEM, SANDHILLS MEDICAL FOUNDATION, INC., and NETGAIN TECHNOLOGY, LLC, Defendants.	Court File No.: _____ **SUMMONS**

THIS SUMMONS IS DIRECTED TO ALLINA HEALTH SYSTEM.

1. YOU ARE BEING SUED. The Plaintiffs have started a lawsuit against you. The Plaintiffs' Complaint against you is attached to this summons. Do not throw these papers away. They are official papers that affect your rights. You must respond to this lawsuit even though it may not yet be filed with the Court and there may be no court file number on this summons.

2. YOU MUST REPLY WITHIN 21 DAYS TO PROTECT YOUR RIGHTS. You must give or mail to the person who signed this summons **a written response** called an Answer within 21 days of the date on which you received this Summons. You must send a copy of your Answer to the person who signed this summons located at:

Raina C. Borrelli
Turke & Strauss LLP
613 Williamson St., Suite 201
Madison, WI 53703
raina@turkestrauss.com

3. YOU MUST RESPOND TO EACH CLAIM. The Answer is your written response to the Plaintiff's Complaint. In your Answer you must state whether you agree or disagree with each paragraph of the Complaint. If you believe the Plaintiff should not be given everything asked for in the Complaint, you must say so in your Answer.

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

4. YOU WILL LOSE YOUR CASE IF YOU DO NOT SEND A WRITTEN RESPONSE TO THE COMPLAINT TO THE PERSON WHO SIGNED THIS SUMMONS. If you do not Answer within 21 days, you will lose this case. You will not get to tell your side of the story, and the Court may decide against you and award the Plaintiffs everything asked for in the complaint. If you do not want to contest the claims stated in the complaint, you do not need to respond. A default judgment can then be entered against you for the relief requested in the complaint.

5. LEGAL ASSISTANCE. You may wish to get legal help from a lawyer. If you do not have a lawyer, the Court Administrator may have information about places where you can get legal assistance. **Even if you cannot get legal help, you must still provide a written Answer to protect your rights or you may lose the case**.

6. ALTERNATIVE DISPUTE RESOLUTION. The parties may agree to or be ordered to participate in an alternative dispute resolution process under Rule 114 of the Minnesota General Rules of Practice. You must still send your written response to the Complaint even if you expect to use alternative means of resolving this dispute.

/s/ Raina C. Borrelli _____ 6/15/2021 _____
Plaintiffs' attorney's signature Dated

Raina C. Borrelli _____
Print or type plaintiffs' attorney's name

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

STATE OF MINNESOTA **DISTRICT COURT**

COUNTY OF HENNEPIN **FOURTH JUDICIAL DISTRICT**

ROBERT SMITHBURG, THOMAS LINDSAY, and ROBIN GUERTIN, individually and on behalf of all others similarly situated, Plaintiffs, v. APPLE VALLEY MEDICAL CLINIC, LTD., ALLINA HEALTH SYSTEM, SANDHILLS MEDICAL FOUNDATION, INC., and NETGAIN TECHNOLOGY, LLC, Defendants.	Court File No.: _____ **SUMMONS**

THIS SUMMONS IS DIRECTED TO APPLE VALLEY MEDICAL CLINIC, LTD.

1. YOU ARE BEING SUED. The Plaintiffs have started a lawsuit against you. The Plaintiffs' Complaint against you is attached to this summons. Do not throw these papers away. They are official papers that affect your rights. You must respond to this lawsuit even though it may not yet be filed with the Court and there may be no court file number on this summons.

2. YOU MUST REPLY WITHIN 21 DAYS TO PROTECT YOUR RIGHTS. You must give or mail to the person who signed this summons **a written response** called an Answer within 21 days of the date on which you received this Summons. You must send a copy of your Answer to the person who signed this summons located at:

Raina C. Borrelli
Turke & Strauss LLP
613 Williamson St., Suite 201
Madison, WI 53703
raina@turkestrauss.com

3. YOU MUST RESPOND TO EACH CLAIM. The Answer is your written response to the Plaintiff's Complaint. In your Answer you must state whether you agree or disagree with each paragraph of the Complaint. If you believe the Plaintiff should not be given everything asked for in the Complaint, you must say so in your Answer.

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

4. YOU WILL LOSE YOUR CASE IF YOU DO NOT SEND A WRITTEN RESPONSE TO THE COMPLAINT TO THE PERSON WHO SIGNED THIS SUMMONS. If you do not Answer within 21 days, you will lose this case. You will not get to tell your side of the story, and the Court may decide against you and award the Plaintiffs everything asked for in the complaint. If you do not want to contest the claims stated in the complaint, you do not need to respond. A default judgment can then be entered against you for the relief requested in the complaint.

5. LEGAL ASSISTANCE. You may wish to get legal help from a lawyer. If you do not have a lawyer, the Court Administrator may have information about places where you can get legal assistance. **Even if you cannot get legal help, you must still provide a written Answer to protect your rights or you may lose the case**.

6. ALTERNATIVE DISPUTE RESOLUTION. The parties may agree to or be ordered to participate in an alternative dispute resolution process under Rule 114 of the Minnesota General Rules of Practice. You must still send your written response to the Complaint even if you expect to use alternative means of resolving this dispute.

/s/ Raina C. Borrelli _____ 6/15/2021 _____
Plaintiffs' attorney's signature Dated

Raina C. Borrelli _____
Print or type plaintiffs' attorney's name

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

STATE OF MINNESOTA **DISTRICT COURT**

COUNTY OF HENNEPIN **FOURTH JUDICIAL DISTRICT**

ROBERT SMITHBURG, THOMAS LINDSAY, and ROBIN GUERTIN, individually and on behalf of all others similarly situated, Plaintiffs, v. APPLE VALLEY MEDICAL CLINIC, LTD., ALLINA HEALTH SYSTEM, SANDHILLS MEDICAL FOUNDATION, INC., and NETGAIN TECHNOLOGY, LLC, Defendants.	Court File No.: _____ **CLASS ACTION COMPLAINT AND JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiffs Robert Smithburg ("Smithburg"), Thomas Lindsay ("Lindsay"), and Robin Guertin ("Guertin") (together, Plaintiffs"), on behalf of themselves and the proposed classes defined below, by undersigned counsel, allege as follows:

NATURE OF THE ACTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Apple Valley Medical Clinic, Ltd. ("Apple Valley Medical"), Defendant Allina Health System ("Allina Health"), Defendant Sandhills Medical Foundation, Inc. ("Sandhills Medical"), and their Information Technology ("IT") service provider, Defendant Netgain Technology, LLC ("Netgain") (together, "Defendants"), arising from their collective failure to

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

safeguard certain Personally Identifying Information[1] and Personal Health Information (collectively "PHI") of hundreds of thousands of healthcare patients. Consequently, those patients' PHI—including their names, dates of birth, Social Security numbers, bank account and routing numbers, billing information, and medical diagnostic information—has been compromised.[2]

2. Apple Valley Medical is a primary- and urgent-care provider in Apple Valley, Minnesota, that contracts with Netgain to host, maintain, and secure Apple Valley Medical's IT

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the breach.

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A "covered entity" is further defined as, inter alia, a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. *Id. Covered entity.* Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. Summary of the HIPAA Privacy Rule, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited May 19, 2021).

Apple Valley Medical, Allina Health, and Sandhills Medical are clearly "covered entit[es]" and some of the data compromised in the Data Breach that this action arises out of is "protected health information", subject to HIPAA. Moreover, a "business associate" includes an entity that, inter alia, provides IT services to or for a covered entity where the provision of the service involves the disclosure of protected health information from such covered entity, or from another business associate of such covered entity, to that IT services provider. *Id. Business Associate*. Netgain, as Apple Valley Medical's, Allina Health's, and Sandhills Medical's IT services provider, is clearly one of Apple Valley Medical's, Allina Health's, and Sandhills Medical's "business associate[s]," and is therefore also subject to HIPAA.

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

system and the data stored in that system. Designated as a "clinic," Apple Valley Medical is part of the Allina Health system of clinics and hospitals.

3. Allina Health is a major healthcare system based in Minneapolis, Minnesota, which owns and operates 12 hospitals and more than 90 clinics throughout Minnesota and western Wisconsin.

4. Apple Valley Medical became part of Allina Health on or about February 4, 2020.

5. On information and belief, at all times relevant to this action, Allina Health was informed that, had full knowledge of, and expressly or impliedly consented to, Apple Valley Medical's contract with Netgain to host Apple Valley Medical's IT system, including patient PHI.

6. Sandhills Medical is a primary care provider in South Carolina, with eight locations spread throughout the state, that contracts with Netgain to host, maintain, and secure Sandhills Medical's IT system and the data stored in that system.

7. Netgain is a St. Cloud, Minnesota-based IT service provider that provides its clients with "cloud-based solutions." In practical terms, Netgain stores its clients' data and information on its network of data centers and Netgain's clients access that data through a "cloud-based" software. Netgain regularly contracts with regional healthcare providers across the country.

8. In or around September 2020, an unauthorized person gained access to Netgain's network (the "Data Breach"), stealing the personal and protected information of hundreds of thousands of individuals, including Plaintiffs.

9. On or about December 4, 2020, Netgain informed Allina Health that the PHI of Apple Valley Medical's patients was part of the information stolen in the Data Breach. The PHI included patient names, dates of birth, Social Security numbers, bank account and routing numbers, billing information, and medical diagnostic information.

10. On or about January 8, 2021, Netgain informed Sandhills Medical that the PHI of Sandhills Medical's patients was part of the information stolen in the Data breach. The PHI included patient names, dates of birth, mailing and email addresses, driver's licenses, Social Security numbers, and claims information which could be used to determine patient diagnoses/conditions.

11. Apple Valley Medical and Allina Health began notifying patients affected by the Data Breach on March 26, 2021. The press release, attached hereto as **Exhibit A**, informed Apple Valley Medical's patients that Apple Valley Medical contracted with Netgain to host Apple Valley Medical's patients' PHI and that their PHI was compromised in the Data Breach (the "Press Release").

12. Sandhills Medical began notifying patients affected by the Data Breach on or about March 5, 2021. The notice of data breach, attached hereto as **Exhibit B**, informed Sandhills Medical's patents that Sandhills Medical contracted with Netgain to host Sandhills Medical's patients' PHI and that their PHI was compromised in the Data Breach (the "Sandhills Notice").

13. Although Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain have not disclosed the number of patients affected, press reports place the number at 157,939 for Apple Valley Medical patients and 39,602 for Sandhills Medical patients. *See* https://www.hipaa.info/third-party-data-breaches-documented-by-apple-valley-clinic-biotel-heart/ (last visited June 14, 2021); https://www.calhipaa.com/healthcare-data-breach-summary-report-for-march-2021/ (last visited June 14, 2021).

14. Plaintiffs, who are longtime patients of Apple Valley Medical and Sandhills Medical, received notice that their PHI was stolen in the Data Breach.

15. Plaintiffs and members of the proposed classes have been significantly injured by the Data Breach due to the reasonable mitigation measures they were forced to employ. Plaintiffs and members of the classes also now forever face an amplified risk of fraud and identity theft due to their sensitive PHI falling into the hands of cybercriminals.

16. On behalf of themselves and the classes preliminarily defined below, Plaintiffs bring causes of action sounding in negligence, breach of contract, breach of the covenant of good faith and fair dealing, violation of the Uniform Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43-48, *et seq.*, violation of the Prevention of Consumer Fraud Act, Minn. Stat. § 325F.68, *et seq.*, trespass to chattels, and unjust enrichment. Plaintiffs seek damages and injunctive and declaratory relief arising from Defendants' failure to adequately protect their highly sensitive PHI.

THE PARTIES

17. Plaintiff Robert Smithburg is a natural person and citizen of the State of Minnesota, residing in Apple Valley, Minnesota.

18. Plaintiff Thomas Lindsay is a natural person and citizen of the State of Minnesota, residing in St. Paul, Minnesota.

19. Plaintiff Robin Guertin is a natural person and citizen of the State of South Carolina, residing in Manning, South Carolina.

20. Defendant Apple Valley Medical Clinic, Ltd. is a domestic business corporation that maintains its principal place of business at 14655 Galaxie Avenue, Apple Valley, Minnesota 55124.

21. Defendant Apple Valley Medical Clinic, Ltd. conducted and/or continues to conduct business at 14655 Galaxie Avenue, Apple Valley, Minnesota 55124.

22. Defendant Allina Health System is a nonprofit domestic corporation that maintains its principal place of business at 2925 Chicago Avenue, Minneapolis, Minnesota 55407.

23. Defendant Allina Health System conducted and/or continues to conduct business at 2925 Chicago Avenue, Minneapolis, Minnesota 55407.

24. Defendant Sandhills Medical Foundation, Inc. is a nonprofit domestic corporation organized under the laws of South Carolina that maintains its principal place of business at 645 South 7th Street, McBee, South Carolina 29101. Sandhills transacts substantial and not isolated business within Minnesota through its contract with Netgain whereby Netgain hosts, maintains, and secures Sandhills Medical's IT system and the data stored in that system from Minnesota.

25. Defendant Netgain Technology, LLC is a Delaware limited liability corporation with its principal place of business located at 720 West Saint Germain Street, St. Cloud, Minnesota 56301.

26. Defendant Netgain Technology, LLC conducted and/or continues to conduct business at 720 West Saint Germain Street, St. Cloud, Minnesota 56301.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction pursuant to Minn. Stat. § 484.01.

28. Venue is proper in this Court because a substantial part of the acts and omissions giving rise to the claims in this action took place in Minneapolis, Minnesota, which is located in Hennepin County and the Fourth Judicial District.

COMMON FACTUAL ALLEGATIONS

A. Plaintiffs and the Classes Entrusted Their PHI to Defendants

29. Plaintiffs and the members of the classes are present and former patients of Apple Valley Medical and Sandhills Medical.

30. As a condition of receiving treatment, Plaintiffs and members of the classes were required by Apple Valley Medical, Allina Health, and Sandhills Medical to confide and make available to them, their agents, and their employees, sensitive and confidential PHI, including, but not limited to, Plaintiffs' and members of the Classes' names, dates of birth, Social Security numbers, bank account and routing numbers, billing information, medical diagnostic information, and other clinical and treatment information related to the care sought there.

31. By obtaining, collecting, using, and deriving a benefit from their patients' PHI, Apple Valley Medical, Allina Health, and Sandhills Medical assumed legal and equitable duties to those individuals and knew or should have known that they were responsible for protecting those individuals' PHI from unauthorized disclosure.

32. Plaintiffs have taken reasonable steps to maintain the confidentiality of their PHI. Plaintiffs, as current patients of Apple Valley Medical and Sandhills Medical, relied on Apple Valley Medical, Allina Health, and Sandhills Medical to keep their PHI confidential and securely maintained, to use this information for business purposes only, and to take reasonable steps to ensure that their vendors would make only authorized disclosures of this information.

33. Indeed, Apple Valley Medical, Allina Health, and Sandhills Medical maintained policies which specifically acknowledge their legal obligations to maintain the privacy of patient PHI entrusted to them and to control the disclosure thereof.

34. Apple Valley Medical's and Allina Health's policy is outlined in the Notice of Privacy Practices (the "Allina Health Privacy Policy"), which was effective April 14, 2003, and was revised on February 25, 2021. *See* Allina Health Notice of Privacy Practices, ALLINA HEALTH, https://www.allinahealth.org/-/media/allina-health/files/customer-service/mn-and-wi-notice-of-privacy-practices.pdf (last visited June 11, 2021).

35. Sandhills Medical's policy is outlined in the Notice of Privacy Practices (the "Sandhills Medical Privacy Policy"), which was effective April 14, 2003, and was last "reviewed" on May 20, 2020. *See* Sandhills Medical Foundation, Inc. Notice of Privacy Practices, SANDHILLS MEDICAL FOUNDATION INC., http://sandhillsmedical.org/wp-content/uploads/2021/03/Notice-of-Privacy-Practices.pdf (last visited June 11, 2021).

36. In the Allina Health Privacy Policy, Apple Valley Medical and Allina Health represent that "We safeguard your health information whenever we use or disclose it," and that "We follow this Notice of Privacy Practices and the law when we use and disclose health information." Allina Health Notice of Privacy Practices, ALLINA HEALTH, https://www.allinahealth.org/-/media/allina-health/files/customer-service/mn-and-wi-notice-of-privacy-practices.pdf (last visited June 11, 2021). The Data Breach that is subject of this civil action is not contemplated or permitted by the Privacy Policy.

37. In the Sandhills Medical Privacy Policy, Sandhills Medical represents that "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Sandhills Medical Foundation, Inc. Notice of Privacy Practices, SANDHILLS MEDICAL FOUNDATION INC., http://sandhillsmedical.org/wp-content/uploads/2021/03/Notice-of-Privacy-Practices.pdf (last visited June 11, 2021). The Data Breach that is subject of this civil action is not contemplated or permitted by the Privacy Policy.

38. Plaintiffs entrusted their PHI to Apple Valley Medical, Allina Health, and Sandhills Medical solely for the purpose of effectuating treatment and the payment therefor with the expectation and implied mutual understanding that Apple Valley Medical, Allina Health, and Sandhills Medical would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

39. Plaintiffs would not have entrusted Apple Valley Medical, Allina Health, and Sandhills Medical with their highly sensitive PHI if they had known that Apple Valley Medical, Allina Health, and Sandhills Medical would entrust it to a vulnerable vendor, such as Netgain, thereby failing to protect it from unauthorized use or disclosure.

B. The Security of Patients' PHI Was Compromised in the Data Breach

40. Mr. Smithburg has been a patient of Apple Valley Medical for approximately 15 years.

41. When Mr. Smithburg presented himself to Apple Valley Medical, its agents prominently posted and/or provided Mr. Smithburg with various disclosure statements regarding the Allina Health Privacy Policy and Apple Valley Medical's and Allina Health's obligations under HIPAA to safeguard patients' PHI—as Apple Valley Medical and Allina Health were required to do so by law. *See, e.g.*, 45 C.F.R. § 164.520(c)(2)(iii)(B).

42. As a condition of receiving treatment, Mr. Smithburg divulged his personal and sensitive PHI to Apple Valley Medical and Allina Health, with the implicit understanding that his PHI would be kept confidential. This understanding was based on all the facts and circumstances attendant to him receiving care, and the express, specific, written representations made by Apple Valley Medical, Allina Health, and their agents.

43. Mr. Lindsay has been a patient of Apple Valley Medical for approximately 40 years.

44. When Mr. Lindsay presented himself to Apple Valley Medical, its agents prominently posted and/or provided Mr. Lindsay with various disclosure statements regarding the Allina Health Privacy Policy and Apple Valley Medical's and Allina Health's obligations under HIPAA to safeguard patients' PHI—as Apple Valley Medical and Allina Health were required to do so by law. *See, e.g.*, 45 C.F.R. § 164.520(c)(2)(iii)(B).

45. As a condition of receiving treatment, Mr. Lindsay divulged his personal and sensitive PHI to Apple Valley Medical and Allina Health, with the implicit understanding that his PHI would be kept confidential. This understanding was based on all the facts and circumstances attendant to him receiving care, and the express, specific, written representations made by Apple Valley Medical, Allina Health, and their agents.

46. Ms. Guertin was a patient of Sandhills Medical for approximately 11 years.

47. When Ms. Guertin presented herself to Sandhills Medical, its agents prominently posted and/or provided Ms. Guertin with various disclosures statements regarding the Sandhills Medical Privacy Policy and Sandhills Medical's obligations under HIPAA to safeguard patients' PHI—as Sandhills was required to do so by law. *See, e.g.*, 45 C.F.R. § 164.520(c)(2)(iii)(B).

48. As a condition of receiving treatment, Ms. Guertin divulged her personal and sensitive PHI to Sandhills Medical, with the implicit understanding that her PHI would be kept confidential. This understanding was based on all the facts and circumstances attendant to her receiving care, and the express, specific, written representations made by Sandhills Medical and its agents.

49. Plaintiffs reasonably relied on Apple Valley Medical's, Allina Health's, and Sandhills Medical's representations to their detriment and would not have provided their sensitive PHI to Apple Valley Medical, Allina Health, and Sandhills Medical if not for Apple Valley Medical's, Allina Health's, and Sandhills Medical's explicit and implicit promises to adequately safeguard that information.

50. With the implied consent of Plaintiffs and members of the classes, Apple Valley Medical, Allina Health, and Sandhills Medical entrusted the PHI at issue in this case to Netgain, an IT service provider that secures, hosts, and maintains its clients' IT systems.

51. According to press reports, as early as September 2020, an unauthorized person used the compromised credentials of a Netgain employee to access Netgain's network and steal the PHI of hundreds of thousands of people. The press reports are attached hereto as **Exhibit C**.

52. On information and belief, Netgain did not discover the breach until November 24, 2020.

53. According to Allina Health, on or about December 4, 2020, Netgain informed Allina Health that the PHI of Apple Valley Medical's patients was part of the information stolen in the Data Breach.

54. On or about January 8, 2021, Netgain informed Sandhills Medical that the PHI of Sandhills Medical's patients was part of the information stolen in the Data breach.

55. Apple Valley Medical and Allina Health began notifying patients affected by the Data Breach through a March 26, 2021, Press Release.

56. Sandhills Medical began notifying patients affected by the Data Breach on or about March 5, 2021, through the Sandhills Notice.

57. Apple Valley Medical and Allina Health's Press Release stated that Apple Valley Medical and Allina Health received confirmation from Netgain on January 29, 2021, that the PHI of Apple Valley Medical's patients was accessed as part of the Data Breach.

58. The Sandhills Notice stated that Sandhills Medical contracted with Netgain to host Sandhills Medical's patients' PHI and that their PHI was compromised in the Data Breach.

59. On or about March 26, 2021, Apple Valley Medical and Allina Health sent letters to affected Apple Valley Medical patients notifying them that their PHI had been compromised during the Data Breach.

60. Sandhills Medical sent letters to affected Sandhills Medical's patients notifying them that their PHI had been compromised during the Data Breach on or about March 5, 2021.

61. Apple Valley Medical, Allina Health, and Sandhills Medical recognized the high likelihood that Plaintiffs and the proposed classes would be victims of identity theft due to the disclosure of their PHI, offering the patients whose PHI was accessed in the Data Breach complimentary one-year identity-theft protection.

62. As a result of the Data Breach, the PHI of 197,541 individuals whose PHI was in the possession of Netgain was compromised.

63. The Data Breach was preventable and a direct result of Netgain's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' PHI.

64. The Data Breach was moreover a direct result of Apple Valley Medical, Allina Health, and Sandhills Medical entrusting Plaintiffs' and class members' PHI to Netgain without conducting reasonable inquiry into Netgain's data security practices.

65. Further, Netgain allegedly discovered the breach on November 24, 2020, but Plaintiffs and the classes were not notified for months, in or around March 2021.

C. The Healthcare Industry is a Prime Target for Cybercriminals

66. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40 percent increase from 2015.[3] The next year, that number increased by nearly 50 percent.[4] The following year the healthcare

[3] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, CyberScout (Jan. 19, 2017), https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last visited June 11, 2021).
[4] *2017 Annual Data Breach Year-End Review*, IRTC, (Jan. 25, 2018),

sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[5]

67. Data breaches within the healthcare industry in general, and with vendors in particular, continued to rapidly increase. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68 percent of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[6]

68. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[7]

69. The PHI stolen in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name and date of birth—is difficult, if not impossible, to change.

---

https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last visited June 11, 2021).

[5] *2018 End-of-Year Data Breach Report*, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-ofYear-Aftermath_FINAL_V2_combinedWEB.pdf (last visited May 19, 2021).

[6] 2019 HIMSS Cybersecurity Survey, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited June 11, 2021).

[7] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXECUTIVE, (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited June 11, 2021).

70. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[8] Likewise, the FBI has warned healthcare organizations that PII data is worth 10 times as much as personal credit card data on the black market.[9]

71. PHI data for sale is so valuable because PHI is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining patient numbers with false provider numbers to file fake claims with insurers.

72. The value of Plaintiffs' PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

[8] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, NETWORK WORLD (Feb. 16, 2015) https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 11, 2021).

[9] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cybercrime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information. *See* Humer, Caroline & Finkle, Jim, Your medical record is worth more to hackers than your credit card, REUTERS, (Sep. 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medicalrecord-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited May 19, 2021). Dark web monitoring is a commercially available service which, at a minimum, Netgain can and should perform (or hire a third-party expert to perform).

73. As storehouses of such lucrative information, vendors like Netgain are also highly targeted by cybercriminals because they lack "sufficient resources to prevent or quickly detect a data breach," making them an easier target.[10]

74. Cybercriminals regularly target the healthcare industry with email phishing schemes, which "remain[] the primary attack vector for nine out of 10 cyberattacks."[11] Apple Valley Medical, Allina Health, and Sandhills Medical did not elaborate on how the Data Breach happened, but since "91% [of] ransomware attacks are the result of phishing exploits…" in the healthcare sector, it is highly plausible that the Data Breach was due to a phishing attack.[12]

75. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

76. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file transfer protocols provide the easiest method to assist employees in properly identifying fraudulent emails and preventing unauthorized access to PHI.

77. From a technical perspective, companies can also greatly reduce the flow of phishing emails by implementing certain security measures governing email transmissions.

---

[10] Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, PONEMON INSTITUTE LLC (May 11, 2016), https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf (last visited June 11, 2021).

[11] Benishti, *supra* note 7.

[12] *Security Report Health Care – Hospitals, Providers and more*, CORVUS INSURANCE 2 (Mar. 3, 2020), https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf (last visited June 11, 2021).

Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

D. Defendants Failed to Sufficiently Protect the PHI Entrusted to Them.

1. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain failed to adhere to HIPAA

78. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[13]

79. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained. *See* 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

80. Moreover, since Apple Valley Medical, Allina Health, and Sandhills Medical are covered entities, and Netgain is their business associate, HIPAA requires that Apple Valley Medical, Allina Health, and Sandhills Medical, inter alia, obtain satisfactory assurances from

[13] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, social security numbers, and medical record numbers.

Netgain that it will appropriately safeguard the PHI Netgain receives or creates on behalf of Apple Valley Medical, Allina Health, and Sandhills Medical. *See* 45 C.F.R. § 164.502(e)(1)(i).

81. The Data Breach itself resulted from a combination of inadequacies showing that Netgain failed to comply with safeguards mandated by HIPAA. Netgain's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Netgain's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

2. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain failed to adhere to FTC guidelines

82. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[14] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain should employ to protect against the unlawful exposure of PHI.

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[15] The guidelines explain that businesses should:

j. Protect the personal customer information that they keep;

k. Properly dispose of personal information that is no longer needed;

l. Encrypt information stored on computer networks;

[14] Start with Security: A Guide for Business, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 11, 2021).
[15] Protecting Personal Information: A Guide for Business, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 11, 2021).

m. Understand their network's vulnerabilities; and

n. Implement policies to correct security problems.

The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

84. The FTC recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's collective failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

87. Moreover, Netgain is required to comply with the Safeguards Rule of the Gramm-Leach-Bliley Act, which requires it to, inter alia:

[16] *See Start with Security*, supra note 14.

a. Designate one or more employees to coordinate its information security program;

b. Identify and assess the risks to client information in each relevant area of the firm's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;

c. Design and implement a safeguards program, and regularly monitor and test it;

d. Select service providers that can maintain appropriate safeguards, making sure their contracts require them to maintain these safeguards; and

e. Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

88. Netgain's failure to adhere to the Safeguards Rule certainly contributed to the Data Breach.

3. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain failed to adhere to industry standards

89. As stated above, the healthcare industry continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018 (363 breaches).[17] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global

[17] 2018 End of Year Data Brach Report, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last visited June 11, 2021).

average of $141 per record.[18] As a result, both the government and private sector have developed industry best standards to address this growing problem.

90. The United States Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[19] DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture."[20] Most notably, organizations must properly encrypt PHI in order to mitigate against misuse.

91. The private sector has similarly identified the healthcare sector as particularly vulnerable to cyber-attacks both because of the of value of the PHI that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[21]

92. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Netgain failed to adopt sufficient data security processes—and Apple Valley Medical, Allina Health, and Sandhills Medical failed to ensure that Netgain implemented those processes—a fact highlighted in the Press Release and the Sandhills Notice

[18] Elizabeth Snell, Healthcare Data Breach Costs Highest for 7th Straight Year, HEALTH IT SECURITY, (June 20, 2018), available at https://healthitsecurity.com/news/healthcare-data-breach-costs-highest-for-7th-straight-year (last visited June 11, 2021).
[19] Cybersecurity Best Practices for Healthcare Organizations, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last visited June 11, 2021).
[20] *Id.*
[21] 10 Cyber Security Best Practices For the Healthcare Industry, ClearVoice (Jun. 18, 2018), https://clearvoice.com/cv/lingwong?id=wpo_9UW8DqUzsgqJtxE8 (last visited June 11, 2021).

which revealed that only after the Data Breach, "We [Apple Valley Medical and Allina Health] are communicating regularly with Netgain to ensure they are taking appropriate steps to better maintain the security of Apple Valley Clinic's data," Ex. A, and "Since the attack, the vendor has implemented additional security measures." Ex. B.

93. Netgain's failure to implement rudimentary security measures made it an easy target for the Data Breach that came to pass.

E. Plaintiffs and the Classes were significantly harmed by the Data Breach

94. As discussed above, PHI is among the most sensitive, and personally damaging information. A report focusing on breaches in the healthcare industry found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000.00" per person, and that the victims were further routinely forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[22]

95. Victims of medical identity theft can suffer significant financial consequences. "In some cases, they [must pay] the healthcare provider, repa[y] the insurer for services obtained by the thief, or . . . engage[] an identity service provider or legal counsel to help resolve the incident and prevent future fraud."[23]

96. Moreover, nearly half of identity theft victims lost their health care coverage as a result of a data breach incident, nearly one-third reported that their premiums went up, and forty percent never resolved their identity theft at all.[24]

---

[22] Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited June 11, 2021).
[23] Fifth Annual Study on Medical Identity Theft, PONEMON INSTITUTE LLC 1 (Nov. 18, 2015), https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 (last visited June 11, 2021).
[24] *Id.*

97. "Unfortunately, by the time medical identity theft is discovered, the damage has been done. Forty percent of consumers say that they found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that thieves incurred in their name. As a result, the consequences of medical identity theft are frequently severe, stressful and expensive to resolve."[25]

98. Moreover, resolution of medical identity theft is time consuming to remedy. "Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident."[26] Consequently, they remain at "risk for further theft or errors in [their] healthcare records that could jeopardize medical treatments and diagnosis."[27]

99. As a result of the Data Breach, Plaintiffs and the classes now face, and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives.

100. As long-standing members of the healthcare community, Apple Valley Medical, Allina Health, and Sandhills Medical knew or should have known the importance of safeguarding patient PHI entrusted to them and of the foreseeable consequences of a breach. Despite this knowledge, however, Apple Valley Medical, Allina Health, and Sandhills Medical failed to ensure that their business associate, Netgain, took adequate cyber-security measures to prevent the ransomware attack from happening.

[25] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, EXPERIAN (Apr. 13, 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited June 11, 2021).
[26] *Medical Idenifty Theft Affected Two Million Victims in 2014*, HELPNETSECURITY, https://bit.ly/35a7Lvi (last visited June 11, 2021).
[27] *Id.*

101. Apple Valley Medical, Allina Health, and Sandhills Medical have offered victims of the Data Breach one year of credit monitoring. But it is incorrect to assume that any semblance of reimbursement to victims of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[28]

102. As a result of Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's collective failure to prevent the Data Breach, Plaintiffs and members of the classes have suffered and will continue to suffer significant damages. They have suffered or are at increased risk of suffering:

a. The loss of the opportunity to control how their PHI is used;

b. The diminution in value of their PHI;

c. The compromise and continuing publication of their PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

[28] Victims of Identity Theft, 2012, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited June 11, 2021).

g. Unauthorized use of stolen PHI;

h. The continued risk to their PHI, which remains in the possession of Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain, is subject to further breaches so long as they fail to undertake the appropriate measures to protect the PHI in their possession; and

i. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and members of the classes.

103. Plaintiffs have already incurred harms as a result of the Data Breach.

104. For example, in an effort to mitigate the heightened risk of identity theft and fraud that they now face, Plaintiffs have expended time and effort in order to mitigate the harm they have suffered on account of the Data Breach.

105. Plaintiff Smithburg has subscribed to a credit monitoring service, which provides him with online credit scores direct from the credit bureaus.

106. Plaintiff Guertin has also subscribed to a credit monitoring service, which provides her with online credit scores direct from the credit bureaus.

107. While these credit monitoring services help Plaintiffs Smithburg and Guertin to determine whether suspicious activity has occurred, they are powerless to stop identity theft in advance. The indemnification and insurance that the credit monitoring services provide is also subject to conditions and exclusions. The credit monitoring services do not eliminate the harm caused by the Data Breach.

108. Indeed, Plaintiff Guertin received an alert from the Social Security Administration that an unauthorized person was trying to use her Social Security number as it relates to her Social

Security benefits. Plaintiff Guertin spends considerable time monitoring her accounts in order to mitigate the harm caused by the Data Breach.

CLASS ALLEGATIONS

109. Plaintiffs bring this class action pursuant to Rule 23 of the Minnesota Rules of Civil Procedure, individually and on behalf of the proposed classes ("Classes") defined as:

> **National Class:** All individuals in the United States whose PHI was compromised as a result of the Data Breach with Netgain Technology, LLC, which was announced by Apple Valley Medical Clinic, Ltd. and Sandhills Medical on March 26, 2021, and March 5, 2021, respectively.
>
> **Minnesota Class:** All individuals in Minnesota whose PHI was compromised as a result of the Data Breach with Netgain Technology, LLC, which was announced by Apple Valley Medical Clinic, Ltd. on March 26, 2021.
>
> **South Carolina Class:** All individuals in South Carolina whose PHI was compromised as a result of the Data Breach with Netgain Technology, LLC, which was announced by Sandhills Medical on March 5, 2021.

110. The following people are excluded from the Classes: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendants or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

111. Plaintiffs and members of the Classes satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties.

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

112. **Numerosity:** The exact number of members of the Classes is unknown but, on information and belief, it is estimated to be over 197,541 and individual joinder in this case is impracticable. Members of the Classes can be easily identified through Defendants' records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

113. **Typicality**: Plaintiffs' claims are typical of the claims of other members of the Classes in that Plaintiffs and members of the Classes sustained damages arising out of Defendants' Data Breach and unlawful practices, and Plaintiffs and members of the Classes sustained similar injuries and damages, as a result of Defendants' uniform illegal conduct.

114. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Classes and have retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Classes. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Classes, and Defendants have no defenses unique to Plaintiffs.

115. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

a. Whether Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain had a duty to protect patient PHI;

b. Whether Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain knew or should have known of the susceptibility of Netgain's systems to a data breach;

c. Whether Netgain's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether Apple Valley Medical's, Allina Health's, Sandhills Medical's, or Netgain's conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unlawful exposure of Plaintiffs' and members of the Classes' PHI;

g. Whether Plaintiffs and members of the Classes were injured and suffered damages or other losses because of Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's failure to reasonably protect Netgain's systems and data network;

h. Whether Plaintiffs and members of the Classes are entitled to relief;

i. Whether Apple Valley Medical, Allina Health, and Sandhills Medical failed to adequately notify Plaintiffs and members of the Classes of the compromise of their PHI;

j. Whether Apple Valley Medical, Allina Health, and Sandhills Medical assumed a fiduciary duty and/or confidential relationship to Plaintiffs and members of the Classes when they entrusted them with their PHI;

k. Whether Apple Valley Medical, Allina Health, Sandhills Medical breached their contracts with Plaintiffs and members of the Classes by failing to properly safeguard their PHI and by failing to properly notify them of the Data Breach;

l. Whether Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain's violation of HIPAA constitutes evidence of negligence;

m. Whether Apple Valley Medical, Allina Health, and Sandhills Medical impliedly warranted to Plaintiffs and members of the Classes that the information technology systems of its business associates were fit for the purpose intended, namely the safe and secure processing of PHI, and whether such warranty was breached;

n. Whether Apple Valley Medical and, Allina Health violated the Minnesota Uniform Deceptive Trade Practices Act (Minn. Stat. §§ 325D.43-48, *et seq.*);

o. Whether Apple Valley Medical and Allina Health violated the Minnesota Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, *et seq.*); and

p. Whether Sandhills Medical violated the South Carolina Data Breach Security Act, S.C. Code Ann. §§ 39-1-90, *et seq*.

116. **Superiority:** This cause is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendants' misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

117. A class action is therefore superior to individual litigation because:

a. The amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the National Class, or Alternatively, On Behalf of Plaintiffs Smithburg, Lindsay, and the Minnesota Class against Apple Valley Medical, Allina Health, and Netgain and On Behalf of Plaintiff Guertin and the South Carolina Class against Sandhills Medical and Netgain)

118. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

119. As a condition of receiving healthcare services, Plaintiffs and members of the Classes were obligated to provide Apple Valley Medical, Allina Health, and Sandhills Medical with their PHI.

120. Plaintiffs and members of the Classes entrusted their PHI to Apple Valley Medical, Allina Health, and Sandhills Medical with the understanding that Apple Valley Medical, Allina Health, and Sandhills Medical would safeguard the PHI.

121. Apple Valley Medical, Allina Health, and Sandhills Medical had full knowledge of the sensitivity of the PHI and the types of harm that Plaintiffs and members of the Classes could and would suffer if the PHI were wrongfully disclosed.

122. Apple Valley Medical, Allina Health, and Sandhills Medical had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, inter alia, designing, maintaining, and testing Netgain's security protocols to ensure that Plaintiffs' and members of the Classes' PHI in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cyber security measures regarding patient PHI.

123. Further, Netgain had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, inter alia, designing, maintaining, and testing its security protocols to ensure that Plaintiffs' and members of the Classes' PHI in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cyber security measures regarding patient PHI.

124. Plaintiffs and members of the Classes were the foreseeable and probable victims of any inadequate security practices and procedures that Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain employed. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain knew of or should have known of the inherent risks in collecting and storing the PHI of Plaintiffs and members of the Classes, the critical importance of providing adequate security of that PHI, that they had inadequately trained their employees, and that their security protocols were insufficient to secure the PHI of Plaintiffs and members of the Classes.

125. Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's conduct created a foreseeable risk of harm to Plaintiffs and members of the Classes. Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's misconduct included, but was not limited to, their failure to take the steps to prevent the Data Breach as set forth herein. Apple Valley Medical's, Allina Health's, and Sandhills Medical's misconduct also included their decision that Netgain would not comply with industry standards for the safekeeping and authorized disclosure of patient PHI.

126. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain, of failing to use reasonable measures to protect PHI. The FTC publications and orders described above also form part of the basis of Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's duty in this regard.

127. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain further violated Section 5 of the FTC Act by failing to use reasonable measures to protect patient PHI and not complying with applicable industry standards, as described herein. Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's conduct was particularly unreasonable given the nature and amount of PHI Netgain obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and members of the Classes.

128. Further, Netgain violated the Safeguards Rule of the Gramm-Leach-Bliley Act by failing to use reasonable measures to protect patient PHI and not complying with applicable industry standards, as described herein.

129. Plaintiffs and members of the Classes had no ability to protect their PHI once they entrusted it to Apple Valley Medical, Allina Health, and Sandhills Medical, who gave the PHI to Netgain.

130. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain have admitted that Plaintiffs' and members of the Classes' PHI was wrongfully disclosed to cybercriminals as a result of the Data Breach.

131. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain breached their duty to Plaintiffs and members of the Classes by failing to exercise ordinary and reasonable care in protecting and safeguarding Plaintiffs' and members of the Classes' PHI while it was within Defendants' possession or control.

132. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain unlawfully breached their duty to Plaintiffs and members of the Classes by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Apple Valley Medical's and Sandhills Medical's patients' PHI.

133. Apple Valley Medical, Allina Health, and Sandhills Medical also unlawfully breached their duty to adequately disclose to Plaintiffs and members of the Classes the existence and scope of the Data Breach.

134. But for Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's wrongful and negligent breach of duties owed to Plaintiffs and members of the Classes, Plaintiffs' and members of the Classes' PHI would not have been compromised.

135. As a result of Apple Valley Medical's, Allina Health's, Sandhills Medical's, and Netgain's negligence, Plaintiffs and members of the Classes have suffered and will continue to suffer damages and injury including, but not limited to, out-of-pocket expenses associated with

mitigating against the heightened risk of identity theft and fraud caused by the Data Breach; the time and costs associated with remedying identity theft and fraud fairly attributable to the Data Breach; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

136. These harms are directly and proximately caused by the Data Breach.

SECOND CAUSE OF ACTION
Breach of Contract Including Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the National Class, or Alternatively, On Behalf of Plaintiffs Smithburg, Lindsay, and the Minnesota Class, against Apple Valley Medical and Allina Health and On Behalf of Plaintiff Guertin and the South Carolina Class against Sandhills Medical)

137. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

138. Apple Valley Medical, Allina Health, and Sandhills Medical offered to provide medical treatment services to Plaintiffs and members of the Classes in exchange for payment.

139. Plaintiffs and members of the Classes accepted Apple Valley Medical's, Allina Health's, and Sandhills Medicals' offer to provide medical treatment services by paying for and receiving said treatment.

140. Apple Valley Medical, Allina Health, and Sandhills Medical required that Plaintiffs and members of the Classes provide their PHI, including dates of birth, Social Security numbers, bank account and routing numbers, billing information, and medical diagnostic information, and other clinical and treatment information related to the care sought there in order to receive care from Apple Valley Medical and Sandhills Medical.

141. Plaintiffs and members of the Classes exchanged valuable consideration—money—with Apple Valley Medical, Allina Health, and Sandhills Medical for services, a crucial

part of which was Apple Valley Medical's, Allina Health's, and Sandhills Medical's implicit promise to protect Plaintiffs' and members of the Classes' PHI from unauthorized disclosure.

142. In the Allina Health Privacy Policy, Apple Valley Medical and Allina Health expressly promised Plaintiffs and members of the Classes that they would only disclose PHI under certain circumstances, none of which relate to the Data Breach.

143. In the Sandhills Medical Privacy Policy, Sandhills Medical expressly promised Plaintiffs and members of the Classes that they would only disclose PHI under certain circumstances, none of which relate to the Data Breach.

144. Necessarily implicit in the agreement between Apple Valley Medical, Allina Health, and Sandhills Medical's patients, including Plaintiffs and members of the Classes, was Apple Valley Medical's, Allina Health's, and Sandhills Medical's obligation to use such PHI for business and treatment purposes only, to take reasonable steps to secure and safeguard that PHI, and not make disclosures of the PHI to unauthorized third parties.

145. Further implicit in the agreement, Apple Valley Medical, Allina Health, and Sandhills Medial was obligated to provide Plaintiffs and members of the Classes with prompt and adequate notice of any and all unauthorized access and/or theft of their PHI.

146. Plaintiffs and members of the Classes would not have entrusted their PHI to Apple Valley Medical, Allina Health, and Sandhills Medical in the absence of such agreement with Apple Valley Medical, Allina Health, and Sandhills Medical.

147. Apple Valley Medical, Allina Health, and Sandhills Medical materially breached the implied contract(s) they had entered with Plaintiffs and members of the Classes by failing to safeguard such information and failing to notify Plaintiffs and members of the Classes promptly of the intrusion into Netgain's computer systems that compromised such information. Apple

Valley Medical, Allina Health, and Sandhills Medical further breached the implied contracts with Plaintiffs and members of the Classes by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Classes' PHI;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PHI that Apple Valley Medical, Allina Health, and Sandhills Medical created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

148. The damages sustained by Plaintiffs and members of the Classes as described above were the direct and proximate result of Apple Valley Medical's, Allina Health's, and Sandhills Medical's material breaches of their agreements.

149. Plaintiffs and members of the Classes have performed as required under the relevant agreements, or such performance was waived by the conduct of Apple Valley Medical, Allina Health, and Sandhills Medical.

150. Under both Minnesota and South Carolina law, good faith is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

151. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

152. Apple Valley Medical, Allina Health, and Sandhills Medical failed to promptly advise Plaintiffs and members of the Classes of the Data Breach.

153. In these and other ways, Apple Valley Medical, Allina Health, and Sandhills Medical violated the duty of good faith and fair dealing.

154. Plaintiffs and members of the Classes have sustained damages as a result of Apple Valley Medical's, Allina Health's, and Sandhills Medical's breaches of its agreements, including breaches thereof through violations of the covenant of good faith and fair dealing.

THIRD CAUSE OF ACTION
Violation of the Uniform Deceptive Trade Practices Act
Minn. Stat. §§ 325D.43-48, *et seq.*
(On Behalf of Plaintiffs Smithburg, Lindsay, and the Minnesota Class, against Apple Valley Medical and Allina Health)

155. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

156. Apple Valley Medical, Allina Health, Sandhills Medical, Plaintiffs, and members of the Classes are all "persons" within the meaning of Minn. Stat. § 325D.44.

157. The Uniform Deceptive Trade Practices Act ("DTPA") prohibits deceptive trade practices, which occur when a person engaged in the course of business in the State of Minnesota.

158. As large healthcare providers, Apple Valley Medical and Allina Health conducted business, trade, or commerce in Minnesota.

159. In the conduct of their business, trade and commerce, and/or in furnishing services in Minnesota, Apple Valley Medical's and Allina Health's actions were directed at consumers.

160. In the conduct of their business, trade, and commerce, and/or in furnishing services in Minnesota, Apple Valley Medical and Allina Health collected and stored highly personal and private information, including PHI belonging to Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class.

161. In the conduct of their business, trade, and commerce, and/or furnishing services in Minnesota, Apple Valley Medical and Allina Health engaged in deceptive, unfair, and unlawful trade acts or practices, in violation Minn. Stat. § 325D.44 including but not limited to the following:

a. Apple Valley Medical and Allina Health misrepresented and fraudulently advertised material facts, pertaining to the sale and/or furnishing of healthcare services to the Minnesota Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs Smithburg's, Lindsay's, and members of the Minnesota Class' PHI from unauthorized disclosure, release, data breaches and cyber-attacks, and moreover, that its business associates would do the same;

b. Apple Valley Medical and Allina Health misrepresented material facts, pertaining to the sale and/or furnishing of insurance, health benefits, and other services, to Plaintiffs Smithburg, Lindsay, and the Minnesota Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to privacy and security of Plaintiffs Smithburg's, Lindsay's, and members of the Minnesota Class' PHI, and that their business associates would do the same;

c. Apple Valley Medical and Allina Health omitted, suppressed, and concealed the material fact of the inadequacy of their business associate, Netgain's privacy and security protections for Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class' PHI;

d. Apple Valley Medical and Allina Health engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiffs Smithburg's, Lindsay's, and members of the Minnesota Class' PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801);

e. Apple Valley Medical and Allina Health engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class in a prompt and accurate manner;

f. Apple Valley Medical and Allina Health engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs Smithburg's, Lindsay's, and members of the Minnesota Class' PHI from further unauthorized disclosure, release, data breaches, and theft; and

162. Apple Valley Medical's and Allina Health's representations regarding the sale and/or furnishing of healthcare services was material to Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class. Apple Valley Medical and Allina Health intended that Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class would rely on these representations and Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class did, in fact, rely on the representations.

163. As a direct and proximate result of Apple Valley Medical's and Allina Health's deceptive trade practices, Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class

suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PHI, and the loss of the benefit of their respective bargains.

164. The above unfair and deceptive practices and acts by Apple Valley Medical and Allina Health were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

165. Apple Valley Medical and Allina Health knew or should have known that Netgain's data systems and data security practices were inadequate to safeguard Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class' PHI and that risk of a data breach or cyber-attack was highly likely. Apple Valley Medical's and Allina Health's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Minnesota Class.

166. The deceptive conduct described herein is ongoing and continues to this date. Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class, therefore, are entitled to relief described below as appropriate for this cause of action.

FOURTH CAUSE OF ACTION
Violation of the Prevention of Consumer Fraud Act
Minn. Stat. § 325F.68, *et seq.*
(On Behalf of Plaintiffs Smithburg, Lindsay, and the Minnesota Class, against Apple Valley Medical and Allina Health)

167. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

168. Apple Valley Medical, Allina Health, Plaintiffs, and members of the Classes are all "persons" within the meaning of Minn. Stat. §§ 325F.68 and 325F.69. Healthcare services is "merchandise" within the meaning of Minn. Stat. §§ 325F.68 and 325F.69.

169. The Prevention of Consumer Fraud Act ("CFA") prohibits "[t]he act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby." Minn. Stat. § 325F.69(1).

170. In the course of its business, Apple Valley Medical and Allina Health violated the CFA by knowingly misrepresenting and falsely advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs Smithburg's, Lindsay's, and members of the Minnesota Class' PHI from unauthorized disclosure, release, data breaches, and cyber-attacks, and moreover, that their business associates would do the same. Apple Valley Medical and Allina Health engaged in one or more of the following unfair or deceptive acts or practices prohibited by the Minnesota CFA:

a. Apple Valley Medical and Allina Health misrepresented material facts, pertaining to the sale and/or furnishing of insurance, health benefits, and other services to Plaintiffs Smithburg, Lindsay, and the Minnesota Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to privacy and security of Plaintiffs Smithburg's, Lindsay's, and members of the Minnesota Class' PHI, and that their business associates would do the same;

b. Apple Valley Medical and Allina Health omitted, suppressed, and concealed the material fact of the inadequacy of their business associate Netgain's privacy and security protections for Plaintiffs Smithburg's, Lindsay's, and members of the Minnesota Class' PHI;

c. Apple Valley Medical and Allina Health misrepresented material facts in failing to disclose the Data Breach to Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class in a prompt and accurate manner; and

d. Apple Valley Medical and Allina Health engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs Smithburg's, Lindsay's, and members of the Classes' PHI from further unauthorized disclosure, release, data breaches, and theft.

171. Apple Valley Medical and Allina Health's scheme and concealment of the true characteristics of their lack of data privacy and security practices and procedures was material to Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class, and Apple Valley Medical and Allina Health misrepresented, concealed, or failed to disclose the truth with the intention that Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class would rely on the misrepresentations, concealments, and omissions. Had they known the truth, Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class would not have purchased healthcare services and/or provided their PHI to Apple Valley Medical and Allina Health or would have paid significantly less for those healthcare services.

172. Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class had no way of discerning that Apple Valley Medical's and Allina Health's representations were false and misleading, or otherwise learning the facts that Apple Valley Medical and, Allina Health had concealed or failed to disclose.

173. Apple Valley Medical and Allina Health, and Sandhills Medical had an ongoing duty to Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class to refrain from unfair

and deceptive practices under the CFA in the course of their business. Specifically, Apple Valley Medical and Allina Health owed Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class a duty to disclose all the material facts concerning the Data Breach because Apple Valley Medical and Allina Health possessed exclusive knowledge. Apple Valley Medical and Allina Health intentionally concealed such material facts regarding the Data Breach from Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class by failing to disclose the true size and scope of the Data Breach after the breach occurred.

174. Plaintiff Smithburg, Lindsay, and members of the Minnesota Class suffered substantial injury as a direct and proximate result of Apple Valley Medical's and Allina Health's concealment, misrepresentations, and/or failure to disclose material information.

175. Pursuant to the CFA, and Minn. Stat. § 8.31(3a), Plaintiffs Smithburg, Lindsay, and members of the Minnesota Class are entitled to relief described below as appropriate for this cause of action.

FIFTH CAUSE OF ACTION
Trespass to Chattels
(On Behalf of Plaintiffs and the National Class, or Alternatively, On Behalf of Plaintiffs Smithburg, Lindsay and the Minnesota Class, against Apple Valley Medical, Allina Health, and Netgain and On Behalf of Plaintiff Guertin and the South Carolina Class against Sandhills Medical and Netgain)

176. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

177. Plaintiffs and members of the Classes entrusted their PHI to Apple Valley Medical, Allina Health, and Sandhills Medical with the understanding that they would keep that information confidential. Apple Valley Medical, Allina Health, and Sandhills Medical transmitted the PHI to Netgain in the course of engaging Netgain's IT services.

178. Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain intentionally dispossessed Plaintiffs and members of the Classes of their PHI and/or used or intermeddled with Plaintiffs' and members of the Classes' possession of their PHI, when it allowed cybercriminals to access it, going far beyond the bounds of any consent Plaintiffs and members of the Classes bestowed upon Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain.

179. Even if Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain did not intentionally dispossess Plaintiffs and members of the Classes of their PHI, Apple Valley Medical, Allina Health, Sandhills Medical, and Netgain knew or believed that due to their failure to follow minimal industry standards and best practices related to the security of their data systems, a data breach like the one that came to pass would be certain.

180. As explained at length above, Plaintiffs and the members of the Classes were damaged thereby.

SIXTH CAUSE OF ACTION
South Carolina Data Breach Security Act, S.C. Code Ann. §§ 39-1-90, *et seq.*
(On Behalf of Plaintiff Guertin and the South Carolina Class against Sandhills Medical)

181. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

182. Sandhills Medical is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

183. Plaintiff Guertin and members of the South Carolina Class entrusted their PHI to Sandhills Medical, and that PHI includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

184. Sandhills Medical is required to adequately notify Plaintiff Guertin and members of the South Carolina Class following discovery or notification of a breach of its data security

program is PHI that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

185. Because Sandhills Medical discovered a breach of its data security program in which PHI that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Sandhills Medical had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

186. By failing to disclose the Data Breach in a timely and accurate manner, Sandhills Medical violated S.C. Code Ann. § 39-1-90(A).

187. As a direct and proximate result of Sandhill Medical's violations of S.C. Code Ann. § 39- 1-90(A), Plaintiff Guertin and the South Carolina Class suffered damages, as described above.

188. Plaintiff Guertin and the South Carolina Class seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

SEVENTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the National Class, or Alternatively, On Behalf of Plaintiffs Smithburg, Lindsay, and the Minnesota Class, against Apple Valley Medical, Allina Health, and Netgain and On Behalf of Plaintiff Guertin and the South Carolina Class against Sandhills Medical and Netgain)

189. Plaintiffs and members of the Classes incorporate the above allegations as if fully set forth herein.

190. In the alternative to the claims alleged above, Plaintiffs allege that they have no adequate remedy at law and bring this unjust enrichment claim on behalf of members of the Classes.

191. Plaintiffs and members of the Classes conferred a monetary benefit on Apple Valley Medical, Allina Health, and Sandhills Medical in the form of payment for healthcare services. Plaintiffs and members of the Classes also provided their PHI to Apple Valley Medical, Allina Health, and Sandhills Medical.

192. The money that Plaintiffs and members of the Classes, directly or indirectly, paid to Apple Valley Medical, Allina Health, and Sandhills Medical should have been used by it, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

193. As a result of Apple Valley Medical's, Allina Health's, and Sandhills Medical's conduct described herein, Plaintiffs and members of the Classes suffered actual damages in an amount equal to the difference in value between healthcare services associated with the reasonable data privacy and security practices and procedures that Plaintiffs and members of the Classes paid for, and the inadequate healthcare services without reasonable data privacy and security practices and procedures that they received.

194. Under principles of equity and good conscience, Apple Valley Medical, Allina Health, and Sandhills Medical should not be permitted to retain money belonging to Plaintiffs and members of the Classes because Apple Valley Medical, Allina Health, and Sandhills Medical failed to use that money to implement the reasonable data privacy and security practices and procedures that Plaintiffs and members of the Classes paid for and that were otherwise mandated by HIPAA regulations, federal and state law, and industry standards and best practices.

195. Apple Valley Medical, Allina Health, and Sandhills Medical should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Classes all unlawful or inequitable proceeds received by Apple Valley Medical, Allina Health, and Sandhills Medical.

196. A constructive trust should be imposed upon all unlawful or inequitable sums received by Apple Valley Medical, Allina Health, and Sandhills Medical traceable to Plaintiffs and members of the Classes.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Classes, request that the Court:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiff Smithburg, Plaintiff Lindsay, and Plaintiff Guertin as the Class representatives, and appoint the undersigned as Class counsel;

B. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Classes;

C. Award injunctive relief as is necessary to protect the interests of Plaintiffs and the Classes;

D. Enter an award in favor of Plaintiffs and the Classes that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

E. Award restitution and damages to Plaintiffs and the Classes in an amount to be determined at trial;

F. Enter an award of attorneys' fees and costs, as allowed by law;

G. Enter an award of prejudgment and post-judgment interest, as provided by law;

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

H. Grant Plaintiffs and the Classes leave to amend this complaint to conform to the evidence produced at trial; and

I. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: June 15, 2021

Respectfully Submitted,

TURKE & STRAUSS LLP

By: /s/ Raina C. Borrelli
RAINA BORRELLI, MN BAR NO. 0392127
SAMUEL J. STRAUSS*

COHEN & MALAD, LLP

By: */s/ Lynn A. Toops*
LYNN A. TOOPS*
LISA M. LA FORNARA*

BRANSTETTER, STRANCH & JENNINGS, PLLC

By:*/s/ J. Gerard Stranch, IV*
J. GERARD STRANCH, IV.*
MARTIN F. SCHUBERT*
PETER J. JANNACE*

* *Pro Hac Vice Admission Forthcoming*

Counsel for Plaintiffs and the Proposed Classes

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

— EXHIBIT A —

651-241-3779

Press Release

Allina Health Apple Valley › Contents › Press Release

Notice of Data Breach from Apple Valley Clinic

MINNEAPOLIS (March 26, 2021) — This notice is regarding a security incident of which the Apple Valley Clinic has become aware. The Apple Valley Clinic provides primary care and urgent care services. The Apple Valley Clinic contracts with Netgain Technology, LLC (Netgain), to host its information technology network and computer systems.

On December 2, 2020, we were notified by Netgain that its systems had been compromised by a cyberattack. After discovering the cyberattack, Netgain notified law enforcement and ultimately regained control of its systems and recovered the affected data. On January 29, 2021 after the Netgain systems were restored, Allina Health received confirmation that the data involved in the cyberattack contained patient data. We have worked with experts to determine what patient data was affected in order to provide our patients with the most accurate information about the incident and the individuals potentially affected.

Data maintained by the Apple Valley Clinic that was involved in the cyberattack on Netgain's system included the following types of personal information:

- Names
- Dates of birth
- Social security numbers
- Bank account and routing numbers
- Patient billing information
- Medical information, such medical symptoms and diagnosis

This incident only impacted individuals receiving health care services at the Apple Valley Clinic. No other Allina locations were impacted by the incident.

We are committed to our patient's privacy and we understand that these types of events can cause concern. Although the Apple Valley Clinic was not targeted in this cyberattack, we are taking steps to enhance our own cybersecurity protocols and practices. In February, we implemented Allina Health's electronic health record system and began migrating the Apple Valley Clinic to a new information technology system, used by Allina Health.

We are communicating regularly with Netgain to ensure they are taking appropriate steps to better maintain the security of the Apple Valley Clinic's data. Netgain has provided written assurances that the threat to its systems has been contained and eliminated. Netgain is continuing to scan its environment to identify potential impacts from the attack and will work promptly to address any new vulnerabilities that may be identified.

In the interest of protecting our patient's privacy, and in accordance with law, Allina Health is in the process of contacting all patients who may have been affected.

We are not aware that any data was disclosed or used by those responsible for the cyberattack. However, out of an abundance of caution, we are offering complimentary identity theft protection services to affected patients of the Apple Valley Clinic.

For More Information. Patients who may have been impacted can call 833-978-2828. Monday – Friday from 8:00 AM to 6:00 PM (Central Time), beginning Monday, March 29, 2021.

Read our FAQs

About Allina Health

Allina Health is dedicated to the prevention and treatment of illness and enhancing the greater health of individuals, families and communities throughout Minnesota and western Wisconsin. A not-for-profit health care system, Allina Health cares for patients from beginning to end-of-life through its 90+ clinics, 11 hospitals, 15 retail pharmacies, specialty care centers and specialty medical services, home care, and emergency medical transportation services.

WHAT WE OFFER

Services

Anticoagulation Clinic more info	Midwifery more info	Chronic Care Management more info	Immunizations more info
Pediatric Wellness more info	Preventive Care more info	Sleep Health more info	Sports Medicine more info
Urgent Care more info	Wellness Visits more info	OBGYN more info	Clinical Skin Therapeutics more info

Allina Health Apple Valley, Apple Valley, MN

Phone (appointments): 651-241-3779 | Phone (general inquiries): 651-241-3779

Address: 14655 Galaxie Avenue, Apple Valley, MN 55124

4.75 / 5 (89 reviews)

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

— EXHIBIT B —

Sandhills Medical Foundation, Inc.

WELCOME TO YOUR PATIENT-CENTERED MEDICAL HOME.

NOTICE:

Notice of Data Breach

At Sandhills Medical Foundation, Inc., we value our patients and their privacy. This notice is to inform our patients about an incident that involved their personal information.

What Happened

Sandhills Medical Foundation, Inc. ("Sandhills") uses an outside vendor to provide electronic data storage for some of its scheduling, billing, and reporting systems. On January 8, 2021, the vendor informed Sandhills that the vendor experienced a ransomware attack that affected Sandhills' systems and the data stored in them. The vendor's investigation showed that the attackers used compromised credentials to access their system on September 23, 2020. The attackers accessed Sandhills' systems on November 15, 2020, and exfiltrated (took) Sandhills' data before the ransomware attack was launched on December 3, 2020.

What Information Was Involved

Sandhills determined that patient medical records, lab results, medications, credit card numbers and bank account numbers were **NOT** affected. The affected data included patient names, dates of birth, mailing and email addresses, driver's licenses, and Social Security numbers. It also included claims information which could be used to determine patient diagnoses/conditions.

What We Are Doing

The vendor reported the attack to law enforcement and hired a cybersecurity firm to investigate and respond to the attack. The vendor paid the attackers to return the data and received assurances that copies of the data were deleted/destroyed. Since the attack, the vendor has implemented additional security measures.

Sandhills reported the breach to the U.S. Department of Health and Human Services, Office for Civil Rights; to the South Carolina Department of Consumer Affairs; and to the national credit reporting agencies. Sandhills sent a letter to each affected patient describing the incident and offering one year of free credit monitoring and identity theft protection.

Learn More

For questions about how to enroll in the free credit monitoring and identity theft protection services, affected patients should call 1-888-236-0854. To speak directly with Sandhills' Compliance Officer about this incident, patients should call 1-800-688-5525.

MISSION

The mission of Sandhills Medical Foundation is to be responsive to community healthcare needs by providing quality, comprehensive, and cost effective healthcare.

COVID ACT NOW

Filed in District Court
State of Minnesota
6/15/2021 10:58 PM

— EXHIBIT C —

Accellion Breach Tally for Centene's Subsidiaries: 1.3M Patients Impacted

The HHS reporting tool shows 1.2M patients of Centene subsidiaries were included in the Accellion FTA hack; a new Netgain victim, vendor incident, and an email hack complete this week's breach roundup.

By Jessica Davis April 06, 2021 - The Department of Health and Human Services' breach reporting tool shows over 1.3 million patients of Centene subsidiaries were impacted by the massive Accellion File Transfer Appliance vulnerability hack and subsequent data exfiltration, first reported in early February.

The incident was reported to HHS in four separate filings, affecting 523,709 Health Net of California patients, 26,637 patients of **Health Net** Life Insurance Company, 686,556 patients of Health Net Community Solutions, and 80,138 California Health & Wellness (**CHW**) patients. All reported entities are subsidiaries of Centene.

The notices show the attackers had access to the entities' information from January 7 until January 25. The impacted data included contact details, dates of birth, insurance ID numbers, and health information, such as treatments and medical conditions.

As previously **reported**, an SEC filing issued by Centene revealed Accellion notified the entity in January 2021 that an attacker exploited multiple, unpatched zero-days vulnerabilities in the FTA platform and combined the flaws with a new webshell called DEWMODE.

The exploit gave the hacker access for a number of days, which resulted in the theft of data from at least 100 Accellion clients, including Centene, Kroger, the Jones Day Law Firm, **Trillium** Community Health Plan, and the Southern Illinois University School of Medicine, among others.

READ MORE: **Dark Web Analysis: Healthcare Risks Tied to Database Leaks, Credentials**

According to an earlier Department of Homeland Security Cybersecurity and Infrastructure Security alert, FIN11 and Clop ransomware threat actors were behind the hack. It's believed initial access began in mid-December. No ransomware was deployed in the incident.

At first, it was unclear the motive of the attack. But Clop actors have since posted troves of stolen data online in a mass extortion effort. A number of impacted entities have also received emails from the attackers, adding to the extortion attempts.

Further, media reports show hackers leaked data purportedly stolen from Stanford University School of Medicine during the Accellion incident. Screenshots shared with *HealthITSecurity.com* show that Clop ransomware actors have also posted data belonging to medical equipment manufacturer Nipro and multiple healthcare-related entities tied to the Accellion hack.

For example, the threat actors previously posted proofs data allegedly stolen from the University of Miami. Among the leaked data set are pages of documents from the Department of Veterans Affairs.

The case demonstrates the extent and reach of the initial Accellion hack, which may remain unclear for the foreseeable future. For now, the impacted entities are continuing to investigate the scope of the incident, as the number of victims continues to rise.

158K APPLE VALLEY CLINIC PATIENTS IMPACTED BY NETGAIN CYBERATTACK

READ MORE: **350M Voicemails, Health Details Exposed by Misconfigured Database**

The number of patients affected by a 2020 cyberattack on Netgain is also on the rise. The latest breach **notification** from Allina Health's Apple Valley Clinic shows that the data of 157,939 patients were compromised by the third-party vendor incident.

At the end of January, reports first revealed that a ransomware attack hit Netgain in September 2020. Attackers leveraged compromised credentials to access the vendor's system, which then spread to a number of client systems.

Access to clients' systems began in November, before the attackers deployed the ransomware payload during the first week of December. Amid the initial attack stages, the hackers also managed to steal some patient data.

Netgain reportedly paid the attackers to recover the stolen data, after receiving "assurances that the attackers deleted the data and did not retain any copies." It's important to note **researchers** have observed hackers providing false evidence of data destruction to then publicly dox victims, even when the ransom is paid.

The vendor has continued to monitor for evidence the attackers may attempt to sell the stolen data. But so far, there's been no evidence of data leakage. As of January 14, Netgain completely contained and eradicated the threat.

READ MORE: **41 States Settle with AMCA Over 2019 Data Breach Affecting 21M Patients**

Apple Valley was notified of the initial cyberattack on December 2. After Netgain recovered from the attack on January 29, the clinic was informed that patient data may have been impacted.

The affected data included patient names, dates of birth, Social Security numbers, bank account and routing numbers, patient billing data, and medical information, like diagnoses and symptoms. The data only included Apple Valley Clinic patients.

In response to the attack, the clinic is enhancing its cybersecurity protocols and practices. The clinic implemented Allina Health's EHR in February and also began migrating the clinic to a new IT system, used by Allina Health, as well.

Apple Valley continues to work with Netgain to ensure the vendor is taking appropriate steps properly secure the patient data in its possession. Netgain is also continuing to scan its environment to identify potential impacts of the attack and to promptly address newly identified vulnerabilities.

Other healthcare entities impacted by the incident include **Sandhills** Medical Foundation (39,602 patients), **Woodcreek** Provider Services (207,000 patients), Elara Caring (100,487 patients), and Minnesota's **Ramsey County** Family Health Division (8,700 residents).

VENDOR INCIDENT LEADS TO YEARLONG BREACH OF BEOTEL PATIENT DATA

BioTel Heart **recently** began notifying 38,575 patients that their data was potentially compromised for about one year, after a vendor inadvertently left personal information exposed online.

In January, BioTel discovered that a vendor failed to secure an online database between October 17, 2019 and August 9, 2020. The impacted information involved medical records collected by the vendor from providers who ordered remote cardiac monitoring services from BioTel.

The affected data included patient names, dates of birth, medical information tied to remote cardiac monitoring services, such as prescribing providers, diagnoses, diagnostic tests, health insurance details, and some SSNs. All patients will receive two years of free identity protection services.

While the notice is scarce on details regarding the leaky database, security researcher Bob Diachenko first **discovered** a database belonging to a medical software company left online without the need for a password or order authorization, in August 2020.

The personal information of more than 3.1 million patients was contained in the database. Around the same time, ***DataBreaches.net*** reported that another researcher found a misconfigured Amazon S3 storage bucket leaking more than 60,000 patient records with PHI tied to the BioTel cardiac network, including scanned faxes of PHI requests from patients whose insurance claims reimbursements were denied. The requests appeared to be handled by SplashRx/HealthSplash.

BioTel has since confirmed that its vendor secured the data stored online and terminated the business arrangement with the vendor responsible for the breach. The entity will also require the vendor to securely delete all copies of BioTel records.

ADVANCED ORTHOPAEDICS PHISHING ATTACK IMPACTS 125K PATIENT RECORDS

The data of 125,291 patients, employees, and dependents was potentially compromised after the hack of multiple email accounts belonging to the Centers for Advanced **Orthopaedics**(CAO) in Bethesda, Maryland.

CAO first discovered unusual activity in its email environment on September 17, 2020 and launched an investigation with assistance from a third-party cybersecurity firm. Officials said they discovered multiple employee accounts were hacked for nearly a year between October 2019 and September 2020.

The investigation determined certain emails were accessible to the attackers during the incident. CAO performed an extensive review and data mining effort to identify the impacted individuals and data.

In January, CAO confirmed protected health information was contained in the accessible emails. Officials said they couldn't confirm if the data was indeed accessed or acquired by the culprit.

The affected data varied by patient but could include medical diagnoses and treatment information, as well as some SSNs, driver's license numbers, passports, financial account details, payment card data, and or emails, usernames, and passwords.

For impacted employees and dependents, the data could include dates of birth, medical diagnoses, treatments, SSNs, and driver's licenses. A smaller subset of individuals may have had passports, financial account details, payment cards, or user credentials impacted, as well.

CAO is reviewing its security policies and procedures, as well as its security infrastructure to prevent a recurrence. Officials said they've also implemented additional safeguards.

NetGain takes data centers offline following ransomware attack

Data centers have been taken down as a 'protective measure'

December 09, 2020 By: Graeme Burton 1 Comment

Managed IT services provider NetGain Technologies has been forced to take some of its data centers offline following a ransomware attack launched in late November.

The Minnesota-based company claims that it took down "a number" of its data centers as a protective measure in an effort to "contain this threat and restore services".

Although NetGain fell victim on 24 November, it was not until Friday 4 December that the company started to email clients, warning them that they may experience "system outages or slowdowns" due to the ransomware attack, according to *Bleeping Computer*. Over the weekend, the company started to shut down data centers in a bid to isolate the ransomware attack and rebuild affected systems.

Rebuilding the domain controllers

In a missive to clients, the company added that it was "running tools and scans to detect, isolate, and clean-up any affected environments" alongside security specialists and experts in post-incident recovery that it had drafted in. However, it remains unable to give clients a firm estimate when it will be able to restore services.

While NetGain has chosen not to release much information to the public, it has been more forthcoming in briefings with clients.

server for malware or other anomalies.

The client added that the attack had targeted the data center operator's domain controllers, which manage networks of thousands of servers, but it also needs to make sure that the attackers have not got any further than that.

Services, added the client, ought to start going back online today following scans, and after other security checks and security updates have been completed. More than 60 staff have been working around the clock to resolve the issue.

The NetGain compromise comes just two months after the internal systems of data center giant Equinix were hit with ransomware. However, in that instance the data centers remained fully operational. In late 2019, a CyrusOne data center was also attacked with ransomware, an attack that ended up affecting six customers.

The NetGain compromise comes as ransomware attackers are starting to up their game with partnership platforms, and streamlining their attack tools to better evade detection. In addition, some have started to exfiltrate data from compromised systems before launching their attacks in order to give themselves extra leverage over their victims.

The attackers then threaten to release sensitive data if their ransom demands are not met. In some instances, companies have been taken down for a month or more.

At the end of December in 2019, global foreign exchange company Travelex was forced to take its systems down throughout January following a ransomware attack launched on New Year's Eve. Customers across the world with foreign exchange tied up in Travelex foreign currency cards were unable to access their cash as a result. Banks that relied upon Travelex to provide foreign exchange were forced to suspend the services.

Travelex management, meanwhile, was roundly criticised for releasing barely any information about the attack for the first two weeks - not even informing the UK's Information Commissioner's Office (ICO) about the attack.

The company reportedly paid a ransom of $2.3 million to the attackers in a bid to restore their systems, but the one-two punch of the ransomware outbreak followed by the drastic reduction in global travel wrought by the global COVID-19 outbreak saw the company collapse into administration in August 2020.

NetGain has not responded to press inquiries about the attack.